REMARKS

Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 11-26 stand rejected under 35 USC 101 as allegedly being directed to non-statutory subject matter. In response, claim 11 has been amended to make more clear its reference in referring to a classifying forwarding element and a decryption forwarding element that receives data from the classifying forwarding element. Since these are physical structures and physically handle a signal, it is respectfully suggested that this claim does in fact represent statutory subject matter.

Claims 11-26 stand rejected under 35 USC 112, second article, as being indefinite. The examiner's diligence in noticing the typographical error is appreciated and this has been obviated.

Claims 1-2, 4-7 and 9-26 stand rejected under 35 USC 102(b) as allegedly being anticipated by Harrison. The claims have been amended to further emphasize their patentable distinctions, and as amended, it is respectfully suggested that the rejection has been obviated.

As pointed out in the rejection, Harrison teaches a basic IPsec a system using a VPN network device. However, in Harrison, the IPsec traffic is all processed in a single device.

As explained column 2, lines 8-20, if the classification parameter is not available, then the VPN device (that is the same device that checks for the key) decrypts the IPsec traffic using the secret key.

This means, that all communications: encrypted and not encrypted, are handled in the same VPN network device in Harrison.

In contrast, the subject matter as now claimed (e.g., claim 1) requires that communications are first received at a classifying forwarding element which determines if the classification parameter is available. If a classification parameter is not available, then the traffic is sent to a second location, effectively downstream of the first location, where it is decrypted. This specific structure has two main advantages. First of all, it offloads the decryption to a separate element. This is not taught or suggested by Harrison. Harrison teaches that the single device does all of the operation, including the decryption.

A second advantage is that the decryption is carried out downstream, only after the classifying forwarding element determines that decryption is necessary and passes it. Since decryption is only carried out after the communication has been already processed, this makes it more difficult for a hacker to hack into this system. A hacker would only get to the front end device - not the device that actually does the decryption. Harrison teaches nothing about this, and therefore these claims should be allowable.

Each of claims 1, 6 and 11 have been amended in this way, and each of these claims should be allowable for these reasons. None of the cited prior art teaches or suggests such a configuration and therefore each of these claims should be allowable.

In view of the above amendments and remarks, therefore, all of the claims should be in condition for allowance. A formal notice to that effect is respectfully solicited

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 12/23/03

Scott C. Harris
Attorney for Intel Corporation
Reg. No. 32,030

Fish & Richardson P.C.
PTO Customer Number: **20985**
12390 El Camino Real
San Diego, CA 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10354455.doc